



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/935,654	08/24/2001	Masahiro Kaminaga	NITT.0027	1059
38327	7590	07/16/2004	EXAMINER	
REED SMITH LLP			DO, CHAT C	
3110 FAIRVIEW PARK DRIVE, SUITE 1400			ART UNIT	
FALLS CHURCH, VA 22042			PAPER NUMBER	
			2124	

DATE MAILED: 07/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/935,654

Applicant(s)

KAMINAGA ET AL.

Examiner

Chat C. Do

Art Unit

2124

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 8/24/01; 01/08/02.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-13 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 August 2001 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
- 1) ☒ Certified copies of the priority documents have been received.
 - 2) ☐ Certified copies of the priority documents have been received in Application No. _____.
 - 3) ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

BEST AVAILABLE COPY

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) /
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 8/24/01; 1/8/02
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

Drawings

1. Figures 1-3 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawing sheets are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

2. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

3. The abstract of the disclosure is objected to because the abstract exceeds 150 words in length, contains legal phraseology "means", and is written in two paragraphs. Correction is required. See MPEP § 608.01(b).

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-13 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Re claim 1, the limitation "in place of the step (1)" in line 6 is unclear whether S_2 must be calculated along with S_1 or S_2 is required to calculate based on the condition selection in step (3). For examination purposes, the examiner disregards the limitation above and considers S_2 must be calculated along with S_1 . The parameters "A", "B", "R", "N", "s", "t", "P", and "g" are indefinite because these parameters are not clearly defined. For examination purposes, the examiner considers these parameters any arbitrary number parameters. In addition, the limitation "properly repeating the above-mentioned steps (1), (2), and (3)" is mis-descriptive because the calculations of S_1 and S_2 are based on only a whole number A, B, and R and the final results are based on only S_1 and S_2 . For examination purposes, the examiner disregards this limitation. Claims 5 and 9 have the same problem.

Thus, claims 2-4, 6-8, and 10-13 are also rejected for being dependent on the rejected base claims 1, 5, and 9 respectively.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

BEST AVAILABLE COPY

Art Unit: 2124

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 1-13 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-13 clearly recite a method for calculating a modular multiplication according to a mathematic algorithm wherein claims 5-8 further include a prime modular factor and claims 9-13 further include polynomials. In order for such a claimed method, computer-related process, or a claimed non-specified apparatus implementing the underlined process to be statutory, the claims must include either a step or means that results in a physical transformation outside the computer or a limitation to a practical application. However, it is clear from the claims that the claims merely recite step or non-specific means for data computation and manipulation in performing a mathematical function. The input is a set of number and output is also a set of number. The claims fail to recite any step or means that results in a physical transformation outside the computer, that includes a limitation to a practical application, or that requires a specific computer to implement the claimed process. Therefore, claims 1-13 are clearly directed to a non-statutory subject matter.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

BEST AVAILABLE COPY

9. Claims 1, 5, and 9 are rejected under 35 U.S.C. 102(b) as being anticipated by Nakada (U.S. 5,961,578).

Re claim 1, Nakada discloses in Figure 5 a tamper-resistant for calculating a modular multiplication, $A*B*R^{(-1)} \bmod N$ (abstract), which appears during crypto-processing (col. 1 lines 10-15), utilizing an information processing device comprising the steps of: a. calculating $S1 = A*B*R^{(-1)} \bmod N$ (e.g. abstract or $CB\{1-2\} = 00$); b. in place of the step (1), calculating $S2 = \{sN + A*(-1)^f\} * \{tN + B*(-1)^g\} R^{(-1)} \bmod N$, (among s, t, f, g, at least one is an integer excepting 0, and f, g are both 0 or 1) (col. 2 lines 23-29 wherein $st = 00$); c. properly selecting the step (1) or (2) (step 4); d. properly repeating the above-mentioned steps wherein finally when the step calculation result selected, for a calculation result S1, $T1 = S1*R^{(-1)} \bmod N$ is calculated to output T1, and when the step (2) is selected, for a calculation result S2, $T2 = S2*R^{(-1)} \bmod N$ is calculated to output $N - T2$ (step 4); and e. using T1 and $N - T2$ as a calculation result of a modular multiplication, $A*B*R^{(-1)} \bmod N$ (abstract).

Re claim 5, it has similar methods of claim 1 wherein modular factor is prime. Thus, claim 5 is also rejected under the same rationale as cited in the rejected claim 1.

Re claim 9, it has similar methods of claim 1 wherein variables are polynomials. Thus, claim 9 is also rejected under the same rationale as cited in the rejected claim 1.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Art Unit: 2124

- a. U.S. Patent No. 5,764,554 to Monier discloses a method for the implementation of modular reduction according to the Montgomery method.
- b. U.S. Patent No. 6,625,631 to Ruehle discloses a component reduction in Montgomery multiplier processing element.
- c. U.S. Patent No. 6,748,410 to Gressel et al. disclose an apparatus and method for modular multiplication and exponentiation based on Montgomery multiplication.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chat C. Do whose telephone number is (703) 305-5655. The examiner can normally be reached on M => F from 7:00 AM to 4:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chaki Kakali can be reached on (703) 305-9662. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Chat C. Do
Examiner
Art Unit 2124

July 9, 2004

Kakali Chaki

BEST AVAILABLE COPY

KAKALI CHAKI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100